

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	
	:	Case Number: 1:12cr120
Plaintiff,	:	
	:	Chief Judge Susan J. Dlott
v.	:	
	:	ORDER DENYING DEFENDANT'S
CHRISTOPHER McGLOWN, JR.,	:	MOTIONS TO SUPPRESS STATEMENTS
	:	AND EVIDENCE
Defendant.	:	

This matter comes before the Court on Defendant Christopher McGlown, Jr.'s Motion to Suppress Evidence/Request for *Franks* Hearing (Doc. 17) and Motion to Suppress Statements (Doc. 18). The Court held a hearing on Defendant's motions. For the reasons that follow, Defendant's Motions are DENIED.

I. BACKGROUND

On November 14, 2012, the grand jury in this district returned an indictment charging Defendant Christopher McGlown, Jr., with the distribution, receipt, and possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(a)(4), 2252(b)(1), and 2252(b)(2). In the present motions, McGlown moves to suppress evidence seized by federal agents pursuant to a warrant issued by Magistrate Judge Bowman during a search of 6624 Lakeside Drive, Apt. 310G, West Chester, Ohio 45069, on November 7, 2012, and statements he made that same date. As grounds for his motion to suppress evidence and request for a *Franks* hearing, McGlown contends that the FBI agent who requested the search warrant included false statements in her supporting affidavit that were material to the magistrate judge's finding of probable cause to issue the warrant. He claims that if the magistrate judge had known information that was

available to the agent, then the search warrant would not have been issued. And although McGlown signed a form waiving his rights under *Miranda*, he claims his statements to the agents were involuntarily made and moves to suppress them.

A. The Search Warrant¹

FBI Special Agent (“SA”) Pamela Kirschner applied for a warrant to search the subject property on November 6, 2012. SA Kirschner supported the application with a twenty-two page affidavit in which she states, inter alia, that there is “probable cause to believe someone using the Internet account registered at 6624 Lakeside Drive, Apt. 310G, West Chester, Ohio has transported, distributed, received, and/or possessed child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A.” Application, Doc. 21-1, at Page ID 93.

SA Kirschner provided the following background information in her affidavit: FBI SA James Zajac, working undercover in Philadelphia, identified internet protocol (“IP”) address 72.49.202.230 as sharing potential child pornography files over a peer-to-peer file sharing network. SA Zajac successfully downloaded six child pornographic videos and two images from that IP address between August 16, 2012 and August 27, 2012. Once he identified the IP address that was the source of the files, SA Zajac discovered the physical address and person associated with the IP address. SA Kirschner’s affidavit explains how SA Zajac determined the physical address associated with the IP address:

23. A query of the American Registry for Internet Numbers online database revealed that IP address 72.49.202.230 was registered to Internet Service Provider Cincinnati Bell Fuse Internet Access. An

¹ Two witnesses testified at the suppression hearing regarding matters relevant to McGlown’s challenge to the search warrant. The Government called SA Kirschner, and Defendant called Cincinnati Bell security officer Debbie Panko.

administrative subpoena was then issued to Fuse Internet Access on 09/17/2012 for the above listed download dates and times.

24. On 09/20/2012, Fuse Internet Access indicated that IP address 72.49.202.230 was assigned to the account registered to Christopher McGlown at the address of 6624 Lakeside Drive, Apartment 310G, West Chester, Ohio 45069, at those dates and times.

Id. at Page ID 106.

SA Kirschner knew certain details about the investigation that she did not include in her affidavit. Specifically, she learned from SA Zajac's report that when Cincinnati Bell security officer Debbie Panko responded via email to the administrative subpoena requesting subscriber information for the IP address 72.49.202.230, she wrote:

Attached are the records you requested. Please call if you have any questions. Unfortunately we are unable to attest to the accuracy of the data. Below is the best information we have available.

Subpoena & Subscriber Information
Christopher McGlown
6624 Lakeside Dr. APT 310G
BTN – 51331006110512

Doc. 21-2, at Page ID 115.² SA Zajac had not previously seen a response from an internet service provider that included the qualifying language, "we are unable to attest to the accuracy of the data," so he followed up with Ms. Panko for more information. As SA Zajac described in his report, Ms. Panko explained to him that "it is standard for [Cincinnati Bell] to state that they could not attest to the accuracy of the results and explained due to ongoing network issues they

² Cincinnati Bell's response to the administrative subpoena, provided by Ms. Panko, is filed as Doc. 21-2 at Page ID 115–120. Those documents were admitted into evidence at the suppression hearing as Gov't Ex. 3.

will occasionally identify the wrong subscriber for an IP address.” Doc. 21-3, at Page ID 121.³

In addition to listing the subscriber information associated with the IP address, Ms. Panko’s email to SA Zajac included five attached files that comprised the records from Cincinnati Bell’s IT department in response to the administrative subpoena. *Id.* at Page ID 116–120. The attachments included information about the electronic devices associated with the IP address and showed that McGlown leased the IP address from July 25, 2012 through September 18, 2012. SA Kirschner’s affidavit in support of the application for warrant to search McGlown’s residence did not mention that Cincinnati Bell could not attest to the validity of the subscriber information and did not specifically reference the documents Cincinnati Bell produced in response to the administrative subpoena.

Also relevant to McGlown’s motion are paragraphs 6(h) and 16 of SA Kirschner’s affidavit. Paragraph 6(h) defines “Internet Protocol address” or “IP address” as “a unique number used by a computer to access the Internet.” Doc. 21-1 at Page ID 98. Paragraph 16 explains the growing phenomenon of peer-to-peer (“P2P”) file sharing and states:

A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This Address, expressed as four sets of numbers separated by decimal points, is unique to a particular computer during an online session. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.

Id. at Page ID 103.

³ SA Zajac’s Form 302 report regarding the investigation and reflecting his follow-up communication with Cincinnati Bell is filed as Doc. 21-3 at Page ID 121. That same document was admitted into evidence at the suppression hearing as Gov’t Ex. 4.

B. The Search⁴

SA Kirschner lead a team of FBI agents and West Chester Police Department detectives in executing the warrant at 6624 Lakeside Drive, Apt. 310G around 6:45 a.m. on November 7, 2012. SA Kirschner testified at the suppression hearing that when the agents entered the apartment, McGlown was asleep on the bed in his bedroom and that a large knife handle was protruding from underneath the mattress. At the foot of McGlown's bed was a laptop computer. Because of the presence of the knife, agents handcuffed McGlown for officer safety.

SA Kirschner took McGlown from the bedroom to the living room, where he sat on the couch. Kirschner explained to McGlown that she had a warrant to search the premises and that he was free to leave if he wanted to. McGlown chose to stay.

SA Kirschner showed McGlown a copy of the search warrant and asked him if he wanted to make a statement. McGlown said he did not. Consistent with this testimony, SA Kirschner's written report states, "[u]pon arrival at McGlown's home to conduct the search warrant, he was asked whether he would be willing to speak to Special Agent (SA) Pamela S. Kirschner and West Chester Police Department (WCPD) Detective David Mize regarding the search. McGlown said no, he wanted to talk to an attorney first." Hr'g Apr. 23, 2013, Def. Ex. 2.

When McGlown declined to speak to SA Kirschner, she returned to the bedroom to continue the search. At that point, she discovered that the laptop computer on McGlown's bed was on and running encryption software. Agents began an onsite forensic review of the

⁴ The Government called the following witnesses to testify regarding the search of McGlown's residence: FBI evidence control technician Lisa Keane; West Chester Police Department Detective Andrew Schweier; West Chester Police Department Detective David Mize; and FBI SA Pamela Kirschner. All were present during the search of McGlown's apartment on the morning of November 7, 2012.

computer. During that review, agents observed that files containing sexually explicit images of children were being uploaded and downloaded. Agents photographed the images on the screen and downloaded the files onto a portable drive. SA Kirschner returned to the living room and told McGlown she knew he had been running encryption software and that the agents had observed child pornography on his computer and were documenting it as evidence. She asked McGlown if this changed his mind about whether he wanted to talk to her. McGlown said he still did not want to talk.

Approximately twenty minutes after SA Kirschner told McGlown that the agents had observed child pornography on his computer and were collecting evidence, McGlown initiated a conversation with West Chester Police Department Detective Andrew Schweier, who was standing near the kitchen table in the combined living room/dining room of the apartment.⁵ McGlown asked Detective Schweier if he should speak to the agents. Detective Schweier told McGlown that was his decision. McGlown asked Detective Schweier if it would benefit him to speak to the agents. Detective Schweier responded that he did not know and that McGlown would have to ask the agents. A few seconds later, McGlown said he wanted to speak to the agents. FBI evidence control technician Ms. Keane, who was sitting at the kitchen table, corroborated this account. She testified that she heard McGlown initiate the conversation with Detective Schweier in which McGlown asked if he should speak to the agents and that she heard

⁵ The Government submitted into evidence a sketch of the interior of the apartment prepared by search team member and FBI evidence control technician Lisa Keane. See Hr'g Apr. 23, 2013, Gov't Ex. 1, also filed as Doc. 21-4. The testimony and the sketch demonstrate that the living room couch is within plain view of and near to the kitchen table. Ms. Keane also prepared an administrative log reflecting the search location, time, and names of team members conducting the search. See Hr'g Apr. 23, 2013, Gov't Ex. 1a.

Detective Schweier tell McGlown that it was McGlown's decision whether or not to talk to the agents.

SA Kirschner testified that because McGlown had previously asserted his right not to speak to her, she took a lot of time talking to him about whether he wanted to talk. She explained to McGlown that he was going to be arrested. She then shared the FBI Advice of Rights form with McGlown. The form states the following:

YOUR RIGHTS

Before we ask you any questions, you must understand your rights.

You have the right to remain silent.

Anything you say can be used against you in court.

You have the right to talk to a lawyer for advice before we ask you any questions.

You have the right to have a lawyer with you during questioning.

If you cannot afford a lawyer, one will be appointed for you before any questioning if you wish.

If you decide to answer questions now without a lawyer present, you have the right to stop answering at any time.

CONSENT

I have read this statement of my rights and I understand what my rights are. At this time, I am willing to answer questions without a lawyer present.

Doc. 22-1, Page ID 132.⁶ SA Kirschner asked McGlown to read the form out loud, which he did. SA Kirschner and Detective Mize witnessed McGlown sign the form at 9:07 a.m. Only then did SA Kirschner begin to interview McGlown. McGlown's interview with SA Kirschner and Detective Mize lasted less than an hour: Ms. Keane noted on the administrative log that at "9 am – suspect wanted to talk" and that the interview stopped at 9:52 a.m.

⁶ The Advice of Rights form was submitted into evidence at the April 23, 2013 suppression hearing as Gov't Ex. 2.

At least three law enforcement personnel were in the room when McGlown signed the Advice of Rights form: Ms. Keane, Detective Mize, and SA Kirschner. All of them testified at the suppression hearing that no one made any threats or promises to McGlown. They also testified that McGlown was comfortable, calm, and coherent; that he seemed to understand the situation; that he never asked to leave; and that at no time during the interview did he ask for the questioning to stop or ask to speak to an attorney. SA Kirschner testified that she believed McGlown to be very smart: he has a bachelor's degree in aerospace engineering and was working toward a masters degree in engineering. The agents and officers involved in the search of McGlown's apartment were armed, but none had a weapon drawn at any time when McGlown was seated on the couch in the living room or during his interview with SA Kirschner and Detective Mize. McGlown was not deprived of food, sleep, or medication during the time law enforcement was conducting the search and subsequent interview.

II. ANALYSIS

A. Motion to Suppress Evidence/Request for *Franks* Hearing

McGlown claims that SA Kirschner's affidavit supporting the application for a warrant to search his residence contains materially false statements that were made knowingly and intentionally, or with reckless disregard for the truth, and that those false statements were necessary to the magistrate judge's finding of probable cause. He argues that the following statements are included in the affidavit and are false: (1) "the IP address 72.49.202.230 is without question associated with the defendant [and] the residence at 66224 [sic] Lakeside Dr., Apt. 310G" (Motion, Doc. 17, at Page ID 43); (2) "'IP address' refers to a unique number used by a computer to access the internet" (*id.* at Page ID 41); and (3) the "IP address identifies the

location of the computer with which the address is associated, making it possible for data to be transferred between computers” (*id.* at Page ID 42). He requests a *Franks* hearing to allow McGlown to challenge the truthfulness of these statements.

In *Franks v. Delaware*, 438 U.S. 154 (1978), the Supreme Court recognized a defendant’s right to challenge the sufficiency of a previously issued and executed search warrant. A defendant is entitled to a *Franks* hearing if he (1) makes a substantial preliminary showing that the affiant knowingly and intentionally, or with reckless disregard for the truth, included a false statement or material omission in the affidavit, and (2) proves that the false statement or material omission is necessary to the probable cause finding in the affidavit. *Franks*, 438 U.S. at 171–72; *United States v. Bonds*, 12 F.3d 540, 568–69 (6th Cir. 1993) (applying the *Franks* doctrine to omissions).

To warrant an evidentiary hearing, a defendant must support allegations of deliberate falsehood or of reckless disregard for the truth with an offer of proof in the form of affidavits or reliable statements of witnesses. *Id.* While material omissions can trigger the need for a *Franks* hearing, “an affidavit which omits potentially exculpatory information is less likely to present a question of impermissible official conduct than one which affirmatively includes false information.” *United States v. Atkin*, 107 F. 3d 1213, 1217 (6th Cir. 1997) (citing *United States v. Martin*, 920 F.2d 393, 398 (6th Cir. 1990)).

If a defendant succeeds in making a preliminary showing that an affiant engaged in “deliberate falsehood” or “reckless disregard for the truth” in supplying a falsehood or omitting information from the affidavit, the Court must then consider the affidavit without the false information or including the omitted portions and determine whether probable cause still exists.

Bonds, 12 F.3d at 568 n.26. If so, no hearing is required. On the other hand, if the affidavit so modified is insufficient to support a finding of probable cause, the defendant is entitled to a *Franks* hearing.

Although McGlown's motion asserts that SA Kirschner's affidavit includes false statements, the issues he brings to light are more fairly characterized as omissions from the affidavit, not false statements. Specifically, McGlown asserts that Kirschner omitted information relevant to two issues: (1) the relationship between an IP address and a subscriber's residential address, and (2) the subscriber information obtained from Cincinnati Bell in response to the administrative subpoena. McGlown did not provide the Court with any affidavits or sworn statements to support his argument that SA Kirschner's affidavit contained deliberate falsehoods or material omissions.

1. File Sharing via an IP address

McGlown's stated concern with the portions of the affidavit that define IP address and provide background information about P2P file sharing is that those portions suggest certainty about the location of a computer that contains evidence of child pornography. He claims it is possible that a computer located *outside the residence* of the IP-address subscriber could use that IP address to receive and distribute child pornography over the internet because multiple computers can access the internet through an IP address associated with a wireless router.

McGlown argues that he had a wireless router and that, accordingly, the child pornographic images that SA Zajac downloaded could have originated from a computer located outside his apartment, say, from a computer in an adjacent apartment. Based on this reasoning, McGlown takes issue with the affidavit's statement that "'IP address' refers to a unique number

used by a computer to access the internet” and “[t]he IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers.” Doc. 21-1 at Page ID 98, 102–03. He argues these statement are false because “the records received by the agents indicated a wireless router was the device associated with IP address 72.49.202.230” (Doc. 17 at Page ID 41) and that the IP address of a wireless router does not disclose the location of the computer that transmitted or received data through that router.

This assertion falls far short of what is required to demonstrate the necessity of a *Franks* hearing. First, McGlown did not demonstrate that the definition of “computer” or the description of P2P file sharing was false. “Computer” is defined in the affidavit as “an electronic, magnetic, . . . or other high speed data processing device performing logical or storage functions, *and includes any . . . communications facility directly related to or operating in conjunction with such device*”—a definition which encompasses a router.⁷ Doc. 21-1 at Page ID 97 (emphasis added). Thus, the affidavit’s statement that “‘IP address’ refers to a unique number used by a computer to access the internet” accurately describes a wireless router accessing the internet.

Second, McGlown did not show that SA Kirschner knowingly omitted information about McGlown’s router. Neither the word “wireless” nor “router” appear in the records produced by Cincinnati Bell in response to the administrative subpoena, so those documents do not expressly

⁷ A “router” is “[a] device, circuit, algorithm, etc., which serves to determine the destinations of individual incoming signals; esp. a device *which receives* data packets *and forwards* them to the appropriate computer network or part of a network.” Oxford English Dictionary (3d ed. 2009) (emphasis added). Thus, it is a “communications facility directly related to or operating in conjunction with” a computer and, therefore, a “computer” as defined in the affidavit. *See* Doc. 21-1 at Page ID 97.

indicate a wireless router was the device associated with the IP address. *See* Doc. 21-2 at Page ID 115-120. While defense counsel claims that SA Kirschner could have looked up the model number of the device listed on the Cincinnati Bell records to determine that the device was a wireless router, no evidence was produced to support this claim.

Even if SA Kirschner had known that the IP address assigned to McGlown was associated with a wireless router and had included that information in her affidavit, the Magistrate would have had probable cause to issue the search warrant. The argument that an IP address is not a sufficient nexus between the sharing of child pornography and a residence has been rejected by the Sixth Circuit. *United States v. Gillman*, 432 F. App'x 513, 515 (6th Cir. 2011).

In *Gillman*, police accessed a P2P internet file sharing network and observed a subject using the IP address 69.138.63.81 possess and share a video showing the sexual exploitation of a minor. *Id.* at 514. A cable communications company indicated that the IP address was assigned to Gillman, who resided at 950 Needham Drive, and a state judge issued a warrant to search the Needham Drive residence based on the officer's affidavit stating that police had obtained child pornography from Gillman's IP address and that Gillman "lived" at the Needham address. *Id.* Gillman argued that the IP address was not a sufficient nexus between the sharing of child pornography and his residence because it was possible he used a wireless internet router—something that would have allowed anyone nearby to access the internet and share child pornography through his IP address.

The Sixth Circuit relied on *United States v. Hinojosa*, 606 F.3d 875 (6th Cir. 2010) to reject the defendant's argument. In *Hinojosa*, the Sixth Circuit held there was a sufficient nexus

between illegality and a defendant's residence where an affidavit established that: (1) child pornography was transferred to police from a specific IP address; (2) that IP address was registered to the defendant's residential address; and (3) the defendant actually lived at that address. *Id.* at 885. The court rejected the defendant's argument that the IP address alone was an insufficient nexus, despite the possibility that IP addresses are not always accessed at their registered residential addresses. *Id.* (citing *United States v. Lapsins*, 570 F.3d 758, 767 (6th Cir. 2009); *United States v. Wagers*, 452 F.3d 534, 540 (6th Cir. 2006)).

Just as in *Hinojosa* and *Gillman*, the IP address here established a sufficient nexus connecting the sharing of child pornography to McGlown's residence and computer. While it is possible that McGlown could have had a wireless router and that someone else could have accessed the network and shared child pornography, "[that] possibility . . . does not negate the fair probability that child pornography emanating from an IP address will be found on a computer at its registered residential address." *Gillman*, 432 F. App'x at 515. Accordingly, the facts included in Kirschner's affidavit—(1) that SA Zajac identified IP address 72.49.202.230 as sharing child pornography files; (2) that Cincinnati Bell indicated that IP address 72.49.202.230 was assigned to the account registered to Christopher McGlown at 6624 Lakeside Drive, Apt. 310G, West Chester, Ohio; and (3) that public records indicated the resident of that address to be Christopher McGlown—established a sufficient nexus connecting the sharing of child pornography to McGlown's residence. That the definition and descriptive portions of SA Kirschner's affidavit do not expressly discuss the possibility that an IP address might be associated with a *wireless* router does not alter that conclusion.

Because McGlown's motion did not sufficiently allege that SA Kirschner engaged in "deliberate falsehood" or "reckless disregard for the truth" with respect to this topic, and because probable cause to issue the warrant would have existed even if the affidavit included information regarding the possibility of another's access to a wireless router, a *Franks* hearing was not required and the Court did not permit defense counsel to examine SA Kirschner about this topic at the suppression hearing.

2. Subscriber Information

In the second prong of his attack on SA Kirschner's affidavit, McGlown argues that SA Kirschner intentionally omitted the fact that Cincinnati Bell could not attest to the accuracy of the information it provided regarding the name and address of the IP address subscriber. He argues that by omitting this information, SA Kirschner's affidavit lead the Magistrate to believe that IP address 72.49.202.230 was without question associated with McGlown and the residence at 6624 Lakeside Dr., Apt. 310G.

A review of the affidavit belies this characterization of its content. In the first page of the affidavit, SA Kirschner states her belief "that *someone using* the Internet account registered at 6624 Lakeside Drive, Apartment 310G, West Chester, Ohio 45069, has transported, distributed, received, and/or possessed child pornography." Doc. 21-1 at Page ID 93 (emphasis added). She supports this statement with the facts that SA Zajac downloaded child pornography files from IP address 72.49.202.230, that Cincinnati Bell "indicated that IP address 72.49.202.230 was assigned to the account registered to Christopher McGlown at the address of 6624 Lakeside Drive, Apartment 310G, West Chester Ohio 45069," and that public records indicate the resident of that address to be Christopher McGlown. Doc. 21-1 at Page ID 106. These statements, taken

together, do not purport to demonstrate that IP address 72.49.202.230 was “without question” associated with McGlown at his residence.

However, the records from Cincinnati Bell did contain information regarding the accuracy of the subscriber data that SA Kirschner did not include in the affidavit. Thus, without deciding whether McGlown had made a substantial showing of intentional or reckless falsity or materiality, the Court agreed to permit McGlown to explore the issue and supplement the record during the suppression hearing.

During the hearing, SA Kirschner testified that she saw Cincinnati Bell’s correspondence in which it indicated it could not attest to the accuracy of the subscriber data. However, she still concluded that there was probable cause to search McGlown’s residence because Cincinnati Bell also stated that the subscriber data was “the best information we have available.” *See* Doc. 21-2 at Page ID 115. SA Kirschner testified that she was further reassured by the response Cincinnati Bell provided to SA Zajac when he followed up on the issue: that it was “standard” for the company to state it could not attest to the accuracy of subscriber data because it “occasionally” identified the wrong subscriber for an IP address due to ongoing network issues. *See* Doc. 21-3 at Page ID 121. She testified that if SA Zajac had not followed up with Cincinnati Bell to get additional information about its inability to attest to the accuracy of the data, then she would have. Ultimately, she concluded from all the information available to her that there was probable cause to believe that someone using the IP address associated with McGlown’s name and address was using the internet to share child pornography. The evidence thus demonstrated that SA Kirschner was aware of the proviso accompanying Cincinnati Bell’s subscriber data and

did not include it in her affidavit. But the mere fact of an omission, without more, does not show recklessness on the part of an affiant. *Bonds*, 12 F.3d at 569.⁸

Even if McGlown had made the preliminary showing that SA Kirschner had acted with deliberate falsehood or reckless disregard for the truth in omitting Cincinnati Bell's proviso from the affidavit, he would not have been entitled to an evidentiary hearing under *Franks* because probable cause to issue the warrant would have existed if the affidavit had included the omitted portions. An affidavit is sufficient to establish probable cause to issue a search warrant when, "given all the circumstances . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Terry*, 522 F.3d 645, 648 (6th Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). "A 'fair probability' is not interpreted as connoting any particular mathematical degree of probability." *Id.* (citing *Maryland v. Pringle*, 540 U.S. 366, 371 (2003)). Thus, while "there must be some nexus between the illegal activity suspected and the property to be searched," the probable cause determination "does not require 'near certainty.'" *Id.* at 648, 649 (citing *United States v. Martin*, 289 F.3d 392, 400 (6th Cir. 2002)).

⁸ McGlown supplemented the record with the testimony of Cincinnati Bell security officer Debbie Panko. Ms. Panko testified that Cincinnati Bell began making the statement "we are unable to attest to the accuracy of the data" as its standard response when, in providing subscriber identification in the context of illegal downloading of copyrighted material under the Digital Millennium Copyright Act, it sometimes identified subscribers that did not have the requested IP address at the particular time in question. Ms. Panko also testified that she had never been notified by a government agent that Cincinnati Bell had provided incorrect subscriber information in response to an administrative subpoena.

McGlown ultimately was unsuccessful in making a preliminary showing that SA Kirschner engaged in deliberate falsehood or reckless disregard for the truth when omitting the Cincinnati Bell proviso from her affidavit. Accordingly, the Court did not need to consider Ms. Panko's testimony in the context of an evidentiary hearing pursuant to the *Franks* doctrine.

When investigating a potential instance of distribution of child pornography over the internet, agents must rely on information provided to them by the internet service providers. That the service provider cannot guarantee its subscriber information with 100% accuracy is not fatal to law enforcement's efforts to obtain a search warrant for the residence of the individual associated with the IP address.

The Sixth Circuit has found that probable cause existed to issue a search warrant in child pornography cases where the link between the suspected illegal activity and the residence to be searched was an individual's email account or "screen name" and the subscriber information for the individual using that account or name. In *United States v. Terry*, the court held that a sufficient nexus existed between an image of child pornography sent by email and the defendant's home computer as was required for probable cause to issue a search warrant. *Terry*, 522 F.3d at 649–50. Even though there were other possibilities, such as a hacker illicitly using the defendant's email account, the district court did not err in concluding that "as a matter of plain common sense, if . . . a pornographic image has originated or emanated from a particular individual's email account, it logically follows that the image is likely to be found on that individual's computer." *Id.* at 648.

Similarly, in *United States v. Wagers*, 452 F.3d 534 (6th Cir. 2006), the Sixth Circuit found there was probable cause to search a home where the defendant had purchased subscriptions to known child pornography websites but where it was unknown which computer he had used to access those sites. And in *United States v. Lapsins*, 570 F.3d 758 (6th Cir. 2009), the Sixth Circuit affirmed the district court's probable-cause finding even though there was "no direct evidence that [the defendant] used a home computer to access his accounts" where the

evidence showed that child pornography was uploaded under the defendant's screen name and in his city of residence. *Lapsins*, 570 F.3d at 767. In short, if absolute certainty were required, then a court would *never* be able to rely on subscriber information regarding an email or IP address. *United States v. Tillotson*, No. 2:08-cr-33, 2008 WL 5140773, at *6 (E.D. Tenn. Dec. 2, 2008). However, "the standard is *probable cause*, not absolute certainty." *Id.*; *see also Gillman*, 432 F. App'x at 515 (holding that an IP address established a sufficient nexus connecting the sharing of child pornography to the defendant's residence and computer and noting that the possibility that someone else could have accessed the defendant's wireless network "[did] not negate the fair probability that the child pornography emanating from an IP address will be found on a computer at its registered residential address.")

In this case, Cincinnati Bell's records indicated that IP address 72.49.202.230 was leased to Christopher McGlown, 6624 Lakeside Dr., Apt. 310G from July 25, 2012 through September 18, 2012. SA Zajac successfully downloaded child pornography from that IP address eight times between August 18, 2012 and August 27, 2012. Even when taking into account the knowledge that Cincinnati Bell occasionally misidentifies subscribers using an IP address at a particular time, the fact that Cincinnati Bell was able to associate a single name and address with the IP address that uploaded child pornography during the relevant time frame created a fair probability that evidence of the suspected illegal activity would be found at McGlown's residence and on his computer. For these reasons, Defendant's Motion to Suppress Evidence/Request for a *Franks* Hearing is denied.

B. Motion to Suppress Statements

McGlown moves to suppress his statements under the Fifth Amendment, which protects a defendant from being “compelled in any criminal case to be a witness against himself.” U.S. CONST. amend. V. Despite having signed an Advice of Rights form indicating that he was willing to answer questions without a lawyer present, McGlown claims that his rights under *Miranda v. Arizona*, 384 U.S. 436 (1966) were violated and that his statements were involuntary. He seeks to suppress his statements on these grounds.

Under *Miranda*, any suspect subjected to a custodial interrogation⁹ must be given notice of his Fifth Amendment privilege against self-incrimination. *Miranda*, 384 U.S. at 478–79. That privilege includes the right to remain silent and also the right to the presence of an attorney. *Id.* at 479. The Fifth Amendment does not absolutely bar law enforcement from questioning a defendant in the absence of counsel. Rather, such questioning is permitted when the defendant has voluntarily, knowingly, and intelligently waived his right to counsel. *Miranda*, 384 U.S. at 444. Whether a waiver constitutes a “knowing and intelligent relinquishment . . . of a known right” depends “‘upon the particular facts and circumstances surrounding [the] case, including the background, experience, and conduct of the accused.’” *Edwards v. Arizona*, 451 U.S. 477, 482 (1981) (quoting *Johnson v. Zerbst*, 304 U.S. 458, 464 (1938)). The Government bears the burden of proving a valid waiver. *Brewer v. Williams*, 430 U.S. 387, 404 (1977).

McGlown was not interrogated by law enforcement personnel until after he had first been advised of his rights under *Miranda* and signed a waiver of those rights. Thus, the only matter for this Court to consider is whether McGlown’s waiver was knowing, intelligent, and voluntary.

⁹ The Government does not dispute that McGlown was subjected to a custodial interrogation.

The totality of the circumstances in this case demonstrate that McGlown's waiver was knowing, intelligent, and voluntary. McGlown invoked his right to remain silent shortly after the agents entered his residence: he told SA Kirschner that he did not want to speak to them and that he wanted to talk to an attorney first. It is undisputed that the agents did not interrogate McGlown at that time but continued their search of his residence. After discovering that the laptop computer in McGlown's bedroom was actively downloading child pornography, SA Kirschner asked McGlown if the discovery "changed his mind." Again, McGlown asserted that he did not want to talk to the agents, and the agents did not question him. Thus, there is no dispute that McGlown initially exercised his right not to speak to the agents without first speaking to an attorney.

Then, approximately twenty minutes later and without any further interaction with law enforcement, McGlown initiated a conversation with Detective Schweier. McGlown asked the detective whether he should speak to the agents. After being advised that the decision was up to him, McGlown said he wanted to speak to the agents.

Once a suspect has expressed a desire to deal with law enforcement only through counsel, he may not be subjected to further interrogation until counsel has been made available to him. *Edwards*, 451 U.S. at 484-85. However, if the suspect *himself* "initiates further communication, exchanges, or conversations with the police," law enforcement may proceed with an interrogation. *Id.* at 485. Under the precedent of *Edwards*, the agents were not barred from interrogating McGlown when he initiated further conversation with them.

After McGlown said he wanted to speak to the agents, SA Kirschner advised him of his rights. McGlown read aloud the Advice of Rights form which stated that he had the rights to

remain silent, to talk to a lawyer before he answered any questions, to have a lawyer present during questioning, and to have a lawyer appointed for him if he could not afford one. SA Kirschner did not begin her interrogation of McGlown until after he had signed the form.

The clear and unequivocal testimony of the law enforcement present at the scene demonstrates that McGlown not only was advised of his rights, but also that he understood those rights and nonetheless chose to continue the interview. Additionally, there is no evidence that the nature of the interrogation was unduly coercive.¹⁰ Accordingly, the Court concludes that McGlown validly waived his Fifth Amendment rights, and the Court finds no ground to suppress McGlown's statements.

III. CONCLUSION

For the reasons stated above, the Court DENIES Defendant Christopher McGlown, Jr.'s Motion to Suppress Evidence/Request for *Franks* Hearing (Doc. 17) and Motion to Suppress Statements (Doc. 18).

IT IS SO ORDERED.

s/Susan J. Dlott
Chief Judge Susan J. Dlott
United States District Court

¹⁰ The Sixth Circuit has established three requirements for a finding that a confession was involuntary due to police coercion:

(i) the police activity was objectively coercive; (ii) the coercion in question was sufficient to overbear the defendant's will; and (iii) the alleged police misconduct was the crucial motivating factor in the defendant's decision to offer the statement.

United States v. Mahan, 190 F.3d 416, 422 (6th Cir. 1999).